IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,	)	
	)	4:11CR3050
Plaintiff,	)	
	)	
v.	)	FINDINGS, RECOMMENDATION,
	)	AND ORDER
KYLE SODERHOLM,	)	
	)	
Defendant.	)	

The defendant has moved to suppress all evidence obtained when defendant's home was searched pursuant to the authority and order of a search warrant. Filing No. 15. The search warrant was signed and issued by the undersigned magistrate judge on January 11, 2011. The defendant does not claim the affiant officer, FBI Special Agent Jeffrey D. Tarpinian, intentionally mislead or concealed material information. He does not claim the judge "rubber-stamped" the warrant, and he does not argue that under the facts presented in the warrant application, no reasonable officer would have relied on the judge's probable cause finding.

The defendant claims the search violated his Fourth Amendment rights because the warrant, on its face, failed to support a finding of probable cause. He claims the warrant application was insufficient because it contained: 1) information obtained by a person who posed as an internet "friend;" 2) statements that were vague, conclusory, and hearsay; and 3) stale information.

For the reasons discussed below, the defendant's motion to suppress evidence found during the search of his home computer should be denied.

THE WARRANT APPLICATION

The application to search defendant's residence at 916 11th Avenue, Holdrege, Nebraska states:

The affiant officer, Special Agent Tarpinian, has twenty-two years of law enforcement experience for the Federal Bureau of Investigation, and has extensive training and experience conducting child pornography investigations. The facts within the warrant affidavit were derived from Tarpinian's own investigation, an investigation performed by FBI Special Agent Barry W. Couch from the Rochester, New York office of the FBI's Buffalo division, and information provided by Nebraska State Patrol Investigators Scott Haugaard and Nathan Malicky. Filing No. 20, at CM/ECF pp. 6, 7 & 18.

On September 17, 2010, SA Couch accessed the internet and launched a publicly available peer-to-peer file sharing program (P2P) from the FBI's Rochester, New York office. Filing No. 20, at CM/ECF p. 17. P2P software can be downloaded from the internet and once installed, can be used to create a network that links the computers of internet users. A P2P network user can choose to share certain computer files, including digital files, with other network users running compatible P2P software. A user can obtain files available from other computers on the network by opening the P2P software on his or her computer, and conducting searches for files currently being shared and available from another user's computer. P2P file-sharing allows parallel file downloads, thereby permitting multiple files to be simultaneously shared and downloaded by another P2P user. Filing No. 20, at CM/ECF pp. 10, 13.

As of January 2011, when the warrant was issued, recently released versions of publicly available P2P software allowed a user to set up a private P2P network, thereby limiting network participants to only those users identified on a private list of "friends." Using this recent version of P2P software, a computer user makes a "friend request," and if the request is accepted, the user is added to a friend list. Files available for sharing can then be accessed and

downloaded directly between the computers of the user making and the user accepting the friend request. Filing No. 20, at CM/ECF p. 13.

A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. The IP address is unique to a specific computer during an online session and facilitates transferring data between computers. Third-party software can be used to identify the IP address of the P2P computer sending the file, and to monitor and log internet and local network traffic. Filing No. 20, at CM/ECF p. 13.

Prior to September 17, 2010, a P2P user with username "Suckboy69" provided his password to SA Couch, thereby allowing SA Couch to view and download from Suckboy69's computer those files which Suckboy69 selected to share with other users. Filing No. 20, at CM/ECF p. 17, ¶ 29 (a). When SA Couch accessed his P2P sharing program on September 17, 2010, he queried his network of friends, and observed that Suckboy69 was logged onto the network. SA Couch browsed Suckboy69's shared folders and saw many images and video files depicting child pornography. Filing No. 20, at CM/ECF p. 17, ¶ 29 (a) .

From the available shared files, SA Couch selected 49 files believed to depict child pornography. Between 2:09 a.m. and 2:31 a.m. (Eastern Standard Time), he downloaded files directly from Suckboy69's computer and while doing so, used a network monitoring program to identify the IP address of the computer. SA Couch discovered that the IP address of the computer was 75.135.246.124. Filing No. 20, at CM/ECF p. 17, ¶ 29 (b) .

According to the American Registry for Internet Numbers (ARIN) online database, IP address 75.135.246.124 was registered to Internet Service Provider Charter Communications. An administrative subpoena served on Charter Communications on September 17, 2010 revealed that at the date and time SA Couch was downloading files containing child pornography from IP address 75.135.246.124, the IP address was assigned to an account

registered to Kyle Soderholm, 916 11th Avenue, Holdrege, Nebraska. Filing No. 20, at CM/ECF p. 17, ¶ 29 (c) .

On September 24, 2010, SA Tarpinian received and reviewed case reports and a CD containing the files downloaded by SA Couch. The CD contained 35 images and one video depicting child pornography. Filing No. 20, at CM/ECF p. 18, ¶ 29 (d) & (e) . Three of the files on the CD had the following names and descriptions:

> 12yo boy cumming.avl This is a twenty-nine (29) second video of a thirteen to fifteen year old naked white male laying on his back on a bed and masturbating his erect penis.
>
> 278_l.jpg This is an image of a eight to ten year old naked white male sitting in a chair and receiving oral sex on his erect penis from a ten to twelve year old white male.
>
> 68178_1218446895.jpg This is an image of an eight to ten year old naked white male kneeling on a bed while receiving oral sex on his erect penis from an eight to ten year old naked white male who is sitting on the bed.

Filing No. 20, at CM/ECF p. 18, ¶ 29 (e) (1-3).

On December 3, 2010, NSP Investigators Haugaard and Malicky, both of whom have extensive training and experience with child pornography investigations, viewed the three image and video files and concluded they depicted "child pornography," (filing no. 20, at CM/ECF pp. 18-19, ¶ 29 (f). The affidavit in support of the warrant application defines child pornography to include:

> [A]ny visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created,

> adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

Filing No. 20, at CM/ECF pp. 8-9, ¶ 6 (b) .

A public records report accessed through Lexis Nexis Accurint, a public records database that can be accessed and searched over the Internet, revealed Kyle Soderholm lived at 916 11th Avenue, Holdrege, Nebraska. Based on the records of the Nebraska Department of Motor Vehicles, 916 11th Avenue, Holdrege, Nebraska was the address on Kyle Soderholm's vehicle registration documents. On December 15, 2010, the United States Postal Inspection Service confirmed that Kyle J. Soderholm was receiving mail at 916 11th Avenue, Holdrege, Nebraska. Filing No. 20, at CM/ECF p. 19, ¶ 29 (g-h) .

Collectors and distributors of child pornography can store images and files on their own computer, or use online resources (including services offered by Internet Portals such as Yahoo and Hotmail) to retrieve and store child pornography collections online. Whether stored online or on a personal computer, if a user has collected child pornography, law enforcement officers can find evidence of the collection by searching the user's computer. A forensic examiner can often recover evidence which shows whether a computer contained P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Filing No. 20, at CM/ECF p. 12, ¶¶ 10-13 . This information is often maintained on the computer indefinitely until overwritten by other data. Filing No. 20, at CM/ECF p. 13, ¶ 13 .

LEGAL ANALYSIS

A search warrant is valid under the Fourth Amendment if it is supported by probable cause. U.S. v. Stevens, 530 F.3d 714, 718 (8th Cir. 2008). When presented with a warrant application, the court must conduct a "'practical, common-sense inquiry,' consider 'the totality of the circumstances set forth,' and determine if, based on the information in the application,

there exists a 'fair probability that contraband or evidence of a crime will be found in a particular place.'" Stevens, 530 F.3d at 718 (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)). A court reviewing a warrant application does not evaluate each piece of information independently, but considers the cumulative meaning of all of the facts. U.S. v. Allen, 297 F.3d 790, 794 (8th Cir. 2002).

The defendant claims his Fourth Amendment rights were violated when SA Couch accessed defendant's P2P shared files using a password provided to SA Couch by "Suckboy69." He claims there was an "implied understanding that Couch was not associated with law enforcement," (filing no. 16, p. 3); "when seeking the password, Couch did not inform the Defendant that he was a law enforcement officer." Filing No. 16, p. 3, n.1. The defendant claims his computer was networked for sharing files with only a few other "friends." Defendant claims he retained a reasonable expectation of privacy that his files would be viewed by only "friends," and although he provided SA Couch with the requisite password, he did not knowingly consent to SA Couch's review of the shared files because SA Couch failed to identify himself as a law enforcement officer.

In essence, the defendant is arguing that undercover law enforcement operations violate the Fourth Amendment. The argument lacks merit. "[I]t has long been acknowledged by the decisions of this Court . . . that, in the detection of many types of crime, the Government is entitled to use decoys and to conceal the identity of its agents." Lewis v. U.S., 385 U.S. 206, 209 (U.S. 1966)(citing Grimm v. United States, 156 U.S. 604, 610 (1895), and Andrews v. United States, 162 U.S. 420, 423 (1896)). A law enforcement officer, in the same manner as a private person, may accept an invitation and enter another's premises for the purposes contemplated by the occupant. Lewis, 385 U.S. at 211.

When SA Couch asked for permission to join the defendant's network of friends, the defendant accepted the request and provided the network password to SA Couch. There is

nothing to indicate SA Couch, by requesting access to the defendant's shared files, entrapped the defendant by convincing or even encouraging the defendant to collect and share child pornography, and there is nothing to indicate SA Couch coerced the defendant to grant his request for file access. SA Couch's undercover access to the defendant's P2P file sharing network did not violate the defendant's Fourth Amendment rights.

The defendant claims probable cause for issuing a warrant was lacking because "there is no information which would indicate that the statements provided by SA Barry W. Couch are reliable and/or trustworthy," (filing no. 16, p. 9, ¶ j). and the affidavit lacked any showing that "the opinion of SA Barry W. Couch is reliable, valid or trustworthy when it comes to identifying child pornography. . . ." Filing No. 16, p. 9, ¶ 10. The defendant argues that "had the information from SA Barry Couch been important or significant, SA Barry Couch could have completed and submitted a sworn affidavit describing his identity, his background, his training and how he came to believe that the Defendant's computer contained child pornography." Filing No. 16, p. 12.

A probable cause showing may be "based on the collective knowledge of all law enforcement officers involved in an investigation and need not be based solely on the information within the knowledge of the officer on the scene if there is some degree of communication." U.S. v. Morales, 238 F.3d 952, 954 (8th Cir. 2001)(quoting U.S. v. Horne, 4 F.3d 579, 585 (8th Cir.1993)). SA Couch is an FBI Special Agent, not an anonymous tipster. When conducting an investigation, a law enforcement officer is entitled to rely upon information provided by other officers without first independently corroborating that information. And based on the totality of the facts presented in the warrant affidavit, SA Couch's information was actually corroborated by other officers. As revealed during SA Tarpinian's review of SA Couch's downloaded files, the description of three of the files indicated they contained images of minors engaged in sexually explicit conduct. Two NSP officers trained to identify child pornography then physically reviewed those three files and

confirmed they contained images of child pornography. Even assuming an FBI Agent's characterization of images as "child pornography" is not, in and of itself, sufficient to support a probable cause showing, (but see, U.S. v. Grant, 490 F.3d 627, 631 (8th Cir. 2007); U.S. v. Koelling, 992 F.2d 817, 822 (8th Cir.1993)), SA Couch's characterization and conclusion was confirmed by the file descriptions and images viewed by other law enforcement officers.

The defendant claims SA Tarpinian's confirmation of child pornography images is insufficient because the affidavit explains his experience with investigating child pornography, but does not indicate he "has been trained to determine what is (and isn't) child pornography." Filing No. 16, p. 13. This assertion is incorrect. The warrant affidavit states SA Tarpinian has specialized training in Online Child Enticement and Child Pornography investigations; he has gained experience in such investigations through training offered by the FBI, the National Center for Missing and Exploited Children (NCMEC), and his on-going work in those areas; he has conducted over 30 search warrants and participated in or generated more than 20 P2P investigations; and through the course of his training and work, he has observed and reviewed "numerous examples of child pornography (as defined in 18 U.S.C. § 2256)." Filing No. 20, p. 6, ¶ 2. SA Tarpinian is abundantly qualified to determine what is (or is not) child pornography.

The defendant claims the warrant affidavit lacks a probable cause showing because it failed to link his computer to the images retrieved by SA Couch. He claims "there is nothing to show how the IP address was determined or how that IP address is, in fact, associated with the computer that housed the alleged child pornography." Filing No. 16, p. 9, ¶ K. This claim lacks merit. The affidavit explains that using third-party software, an officer can monitor a network and identify the IP address of a computer sending a file with P2P sharing software, (filing no. 20, p. 13, ¶ 18), and while downloading shared files on September 17, 2010, "SA Couch used a network monitoring program in order to identify the IP address." Filing No. 20,

p. 17, ¶ 29(b). Considered in the totality, the affidavit describes how the officer identified the IP address of the computer being operated under the username "Suckboy69."

The defendant claims that even if the IP address identified by SA Couch was correct, the warrant affidavit lacked a sufficient showing to link that computer to the defendant because it contained nothing to indicate the "American Registry of Internet Numbers" database is a reliable source for obtaining IP address information. Filing no. 16, p. 10, ¶ M. As stated in the affidavit, ARIN is a self-described nonprofit organization responsible for managing the Internet numbering resources for North America, and a portion of the Caribbean. Filing No. 20, p. 18, ¶ 29(c). In the context currently before this court, ARIN (like the Postal Service, Lexis/Nexis Accurint, and the Nebraska Department of Motor Vehicles), served as a "citizen informant;" it provided information deemed reliable for the purposes of determining probable cause because it has no motive to provide false information. U.S. v. Ross, 713 F.2d 389 (8th Cir. 1983). The warrant affidavit is not defective because it failed to state a basis for concluding ARIN is a reliable source of IP address information.

Although the defendant claims otherwise, the warrant affidavit also included information describing the link between the IP address and the defendant. Filing No. 16, p. 10, ¶ M. The affidavit explains that Charter Communications was the identified ISP provider for IP address 75.135.246.124, and in response to an administrative subpoena, Charter Communications stated that at the date and time files were being downloaded by SA Couch from IP address 75.135.246.124, that IP address was assigned to an account registered to the defendant at 916 11th Avenue, Holdrege, Nebraska. Filing No. 20, at CM/ECF p. 17, ¶ 29 (c).

The defendant claims the affidavit includes vague, conclusory, irrelevant, and boilerplate information, and in the absence of this information, there was no showing of probable cause. The facts within the affidavit, and the conclusions derived from those facts, were provided by a highly trained and very experienced law enforcement officer, FBI Special

Agent Tarpinian. See filing no. 20, at CM/ECF p. 6, ¶¶ 1 & 2. While some of the facts within the affidavit may not have been directly relevant to an application to search the defendant's computer, (see e.g., filing no. 20, at CM/ECF p. 12, ¶ 9; p.16, ¶¶ 24-28), even excluding these paragraphs, SA Tarpinian's affidavit provided a basis for believing the defendant's computer contained evidence that the defendant was or had received, collected, and distributed child pornography.

And many of the paragraphs the defendant describes as irrelevant are actually relevant to the finding of probable cause, particularly as it relates the defendant's claim that the warrant application information was "stale." Paragraphs 10, 11 and 12, labeled irrelevant by the defendant, explain how persons interested in viewing child pornography can use computer and online sources to review, collect, distribute and trade child pornography in a relatively anonymous fashion. As explained in paragraph 13, such information (or at least traces of it) will often remain on the computer "indefinitely until overwritten by other data." Filing No. 20, p. 13, ¶ 13 (emphasis added). A forensic examination may disclose whether P2P software was installed, whether and when files were shared, and the content of some of the files that were uploaded and downloaded from the computer. Although SA Couch's discovery of child pornography on defendant's computer occurred in September 17, 2010, this information was not "stale" and provided a reasonable basis for concluding information would likely be found on the computer identified to IP address 75.135.246.124 during a search conducted in mid-January of 2011. U.S. v. Estey, 595 F.3d 836, 840 (8th Cir. 2010)(holding a search warrant issued five months after discovering information linking the defendant's residence with child pornography was valid; "evidence developed within several months of an application for a search warrant for a child pornography collection and related evidence is not stale").

Based on the totality of information presented, SA Tarpinian's affidavit provided a sufficient basis for concluding there was probable cause to search the defendant's home for evidence of child pornography. And even if probable cause was lacking, the defendant has

made no showing that the affiant officer intentionally or recklessly misstated or omitted material facts in his warrant application, that the undersigned judge completely abandoned her judicial role when issuing the warrant, or that a reasonable officer would not have relied on the warrant as authority to perform the search. Franks v. Delaware, 438 U.S. 154 (1978); U.S v. Hessman, 369 F.3d 1016, 1019 (8th Cir. 2004). The evidence found in defendant's residence during a search conducted pursuant to the warrant issued by the undersigned magistrate judge is admissible under the good faith exception set forth in U.S. v. Leon, 468 U.S. 897 (1984).

An evidentiary hearing is not necessary and will not be held on defendant's challenge to the warrant application. The defendant's motion to suppress the evidence found during the search of his residence and home computer should not be suppressed.

IT THEREFORE HEREBY IS RECOMMENDED to the Honorable Warren K. Urbom, United States District Judge, pursuant to 28 U.S.C.§636(b)(1)(B), that the defendant's motion to suppress, (filing no. 15), be denied in all respects.

The parties are notified that a failure to object to this recommendation in accordance with the local rules of practice may be held to be a waiver of any right to appeal the district judge's adoption of this recommendation.

IT IS ORDERED: A hearing will not be held on defendant's motion to suppress the evidence found during the search of his home, (filing no. 15), but the hearing on defendant's motion to suppress statements, (filing no. 17), remains scheduled to be held before the undersigned magistrate judge on September 28, 2011 at 9:00 a.m.

September 26, 2011. BY THE COURT:

s/ Cheryl R. Zwart
United States Magistrate Judge

*This opinion may contain hyperlinks to other documents or Web sites. The U.S. District Court for the District of Nebraska does not endorse, recommend, approve, or guarantee any third parties or the services or products they provide on their Web sites. Likewise, the court has no agreements with any of these third parties or their Web sites. The court accepts no responsibility for the availability or functionality of any hyperlink. Thus, the fact that a hyperlink ceases to work or directs the user to some other site does not affect the opinion of the court.